If we use ubuntu virtual box we can take advantage of linux auditing.

When other user try to tamper our repository folder and file that will be recorded to audit.

Uploaded rutgers-isn-disk2.zip (provided in email dt 4/15 as google drive link)

Unzip that file to rutgers-isn-disk2.vdi (5GB)

Download Oracle VM Virtual Box manager and attach vdi file.

Start virtual machine to get login prompt.

Login as cs419/admin

Audit commands

auditctl -w /home/cs419/PROJ/.SYSSEC/ -k proj\_watch

auditctl -l

ausearch -k proj\_watch

We can login as following user

Cs419 for sercurity system project

Alice and bob to validate correct user

User:hacker try to tamper the system

Login details of virtual box

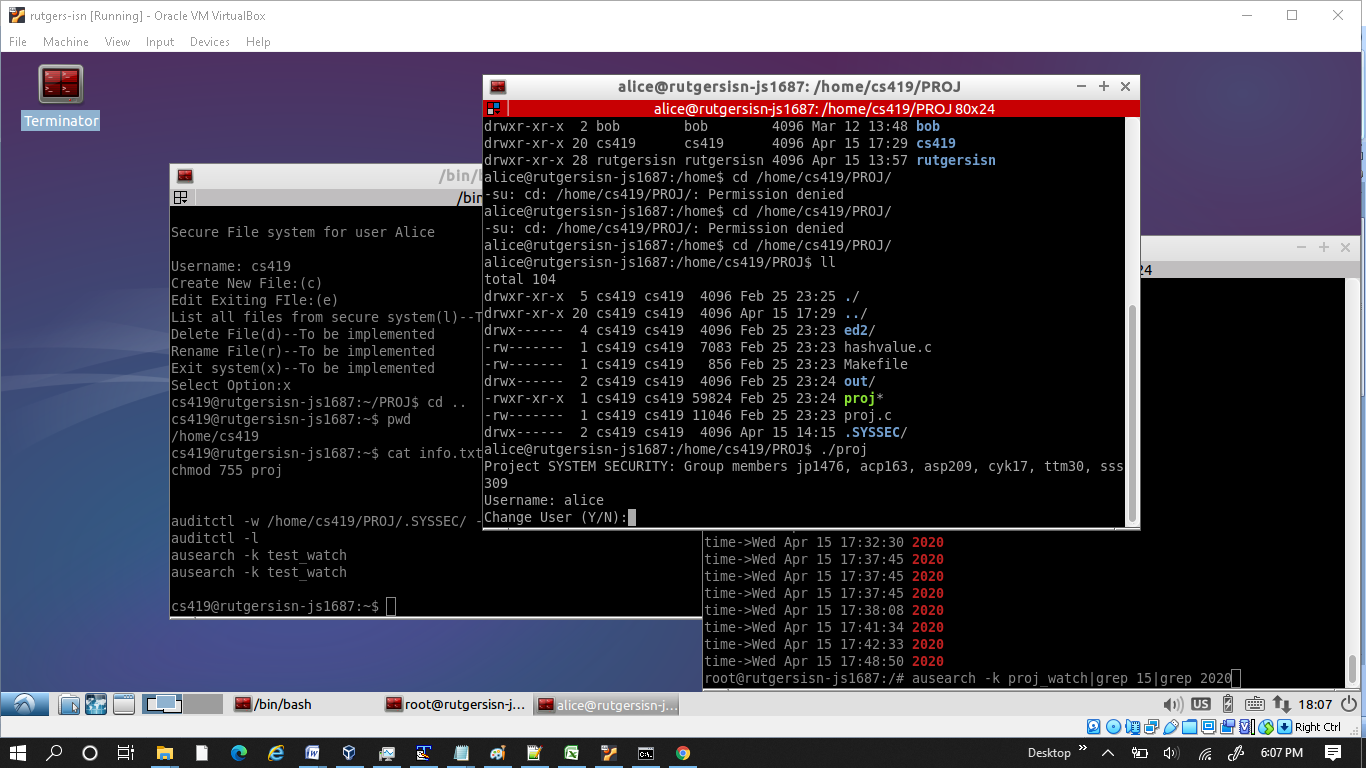
Username:cs419 pwd:admin

Username:su and sudo pwd admin

username:alice pwd:alice

username:bob pwd:bob

username:hacker pwd:hacker



3 terminal windows for user cs419, alice and su to run ausearch (audit search)

Project directory is

/home/cs419/PROJ

No change in code, it is same as 0225 proj.tar file.